Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organisation

Ying He[*1], Chris Johnson[2]

[1]*School of Computer Science and Informatics, De Montfort University, UK*

[2]*School of Computing Science, University of Glasgow, UK*

Corresponding author: ying.he@dmu.ac.uk (Ying He)

Challenges of Information Security Incident Learning: An Industrial Case Study in a Chinese Healthcare Organisation

Security incidents can have negative impacts on healthcare organisations and the security of medical records has become a primary concern of the public. However, previous studies showed that organisations had not effectively learned lessons from security incidents. Incident learning as an essential activity in the "follow-up" phase of security incident response lifecycle, has long been addressed but not given enough attention. This paper conducted a case study in a healthcare organisation in China to explore their current obstacles in the practice of incident learning. We interviewed both IT professionals and healthcare professional. The results showed that the organisation did not have a structured way to gather and redistribute incident knowledge. Incident response was ineffective in cycling incident knowledge back to inform security management. Incident reporting to multiple stakeholders faced a great challenge. In response to this case study, we suggest the security assurance modelling framework to address those obstacles.

Keywords: information security, incident response, incident learning, healthcare, security assurance modelling

1. Introduction

Security incidents have affected healthcare organisations across the world, such as Veterans Affairs' data loss incidents [1, 2] in North American, National Health Service (NHS) Surrey IT asset disposal incident in UK [3] and Shenzhen hospital's data loss incident [4] in China. Industry reports indicated that the number of security incidents happened in healthcare organisations was increasing. Symantec reports showed that the healthcare industry accounts for 36\% of the total security incident breaches in UK in 2013 [5]. At 44\%, the healthcare industry continued to be the sector responsible for the largest percentage of disclosed data breaches by industries in 2014 [6].

A patient's medical record is a collection of personal information including

“identification, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income, and physicians’ subjective assessments of personality and mental state among others” [7, 8]. Healthcare information security has become a primary concern of the public [9-16]. Waegemann claimed that the disclosure of a patient's medical record could ruin or damage an individual's career, and result in dismissal from work, and loss of health insurance [17]. Data loss incidents can also cause financial loss to healthcare organisations. Healthcare organisations will be fined if they failed to protect patients' personal information. For instance, the healthcare organisations in UK were fined hundreds of thousands pounds following data breaches affecting thousands of patients and staff [18-20].

Security incident response is the process that aims to minimise the damage from security incidents and learn from such incidents. There are well-documented methodologies such as the SANS [21] and NIST SP800-61 models [22] that divide this process into several distinct phases including preparation, identification, containment, eradication, recovery and follow-up. A key activity in the “follow-up” phase is the capacity to learn from the errors or mistakes made throughout the incident handling process, to learn about the effectiveness of security policies, procedures, technical processes and to feed this knowledge back into the “preparation” phase [22]. The response to these lessons learned should ideally cycle relevant knowledge and changes into the procedures that guide incident response and result in changes in the training processes and incident response policies. However, case studies [23-25] showed that incident learning is ineffective in the organisations.

During the “follow up” phase, the recommendations and insights derived from previous security incidents should be disseminated through a series of formal and informal reports, meetings and presentations to management [21, 26]. Lessons learned

to document included the effects of the damage, actions taken during the incident, policies and procedures that required a change and evidence that can be used for pursuing the responsible person [21] Previous research showed that security lessons had not been effectively learned within the organisations. For example, a series of case studies [23] performed in the financial organisations showed that risk assessment processes in the organisations were not informed by data on previous incidents including impact and probability of occurrence, and there is a lack of communication between related security functions in the organisations. We have not found any business case study in incident learning in healthcare organisations.

In UK and North America, there were some initiatives such as incident reporting to encourage incident learning. The objective was to reduce the recurrence both where the original incident occurred and elsewhere. In China, little study can be found regarding incident learning as information security was not the main concern of the healthcare providers and governments [27, 28] in the past. Until recently, Chinese healthcare organisation started to realise the importance of healthcare information security. Health information security was stressed in the Management Measures for Population Health Information (for Trial Implementation), issued May 5, 2014 by China's National Health and Family Planning Commission of China. This paper conducts an industrial case study in a Chinese healthcare organisation to investigate their challenges and obstacles in incident learning. It will then present a model to address the identified challenges.

The remainder of the paper is structured as the following. Section 2 reviews related work. Section 3 introduces the industrial case study. Section 4 reports the results of the case study. Section 5 discusses the findings and proposes the security assurance

modelling framework to address the problems identified in the case study. Section 6 summarises the conclusions and identifies future directions.

2. Related work

2.1 Lessons learned and Security Incident Response and Handling (SIRH)

Security Incident Response and Handling (SIRH) can be defined as "the process that aims to minimise the damage from security incidents and malfunctions, and monitor and learn from such incidents" [29]. There were well-structured models provided by SANS, NIST and ISO 27035 models consisting of several distinct phases to isolate an incident and appropriately respond to it, including preparation, identification, containment, eradication, recovery and follow-up [30]. A "follow-up" phase is an essential stage of the SIRH. A key activity in this phase is to learn from the errors or mistakes made during the incident. It is important to identify policies and processes that undermine existing defences. It is also important to identify any weaknesses in staff competency. These insights must then be fed back into security management procedures [21, 26].

Although standard incident response models put an emphasis on incident learning, organisational practices in incident response were still limited to the technical process and were not very engaged in post-incident learning activities. The case studies performed by Ahmad showed that the organisation had focused on improving the technical aspects and did not leverage opportunities to learn about incidents [24, 25]. He then proposed a double-loop model for incident learning [24] and a dynamic security learning (DSL) process model elaborating different learning activities in different learning stages, key stakeholders involved and its linkage with broader organisational

aims [25]. Tondel [31] had identified the key challenges of incident learning which included the lack of willingness to share incident learning with other organisations [32] ineffective communication between IT professionals and other stakeholders [32] the lack of incident learning motivations [32] as well as the insufficient sharing of security lessons within the organisation [23].

2.2 Lessons learned dissemination

Traditional ways to disseminate lessons learned about an incident included a series of formal reports, emails, newsletters, meetings and presentations to management [26, 33]. For example, NHS shared and disseminated lessons learned from security incidents using team meetings, notice boards, incident reporting and investigation training courses (e.g. use of case studies), emails, newsletters, internal alert systems and so on [34]. Emails, newsletters, meetings and presentations to management contained less information comparing to the formal post-incident reports. Post-incident reports documented information obtained throughout the security incident investigation process. Example post-incident reports included the VA data loss incidents [1, 2] from the US, the NHS IT asset disposal incident [35] from UK. They provided a reference that can be used to assist in handling similar incidents [26, 36]. Contents included the causes of the incident, the recommendations on remediation, the security requirements violated and improvements on procedures. Although this information was inter-related, details can be scattered throughout a report, which resulted in ineffective communication of security lessons [37]. This problem has been compounded by usually lengthy written security incident reports, which can be hundreds of pages [1, 2].

2.3 Lessons learned dissemination in healthcare

In Europe and North America, there were some initiatives in encouraging the dissemination of lessons learned in the aftermath of security incidents. In the US, the security incidents were reported to Nation's Healthcare and Public Health Information Sharing and Analysis Centre (NH-ISAC). In UK, NHS report Serious Untoward Incidents that involved the unauthorised disclosure of confidential patient information to the Caldicott Guardian [38] the Senior Information Risk Owner (SIRO) and the relevant Information Asset Owner for consideration of any actions [34]. A Serious Untoward Incident related to Personal Identifiable Data was defined as "the actual or potential loss of personal data and/or any information that could lead to identity fraud or have other significant impact on individuals or the organisation" [34]. The key aim of serious incident reporting was to reduce the recurrence both where the original incident occurred and elsewhere [34]. In China, there have not been requirements found for healthcare organisations to report security incidents and learn from lessons. Health information security has not attracted significant attention by the healthcare providers and governments [27, 28] in the past few years, although some attempts have been made to protect health information [39-42]. Gao suggested two main reasons for the lack of motivations: (1) the Chinese traditional culture does not address the importance of personal privacy; and (2) healthcare systems in China are still in their infancy and there has not been large-scale health data exchange that can potentially trigger large amounts of serious privacy violations [43]. However, the implementation of healthcare information systems can hardly be successful if health information security cannot be ensured [44].

3. The exploratory industrial case study

This section conducted an industrial case study with people working in a healthcare

organisation in China. The objective was to have a deeper understanding of security incident learning practices in healthcare organisations. In particular, we investigate into the obstacles and challenges in incident learning within this organisation.

3.1 Background

A five months internship was accepted in 2013, with a Chinese healthcare organisation, the redacted hospital, on a newly initiated Security Strengthening Program (SSP). The redacted hospital started using an electronic healthcare system from 2008 and was looking for recommendations to improve their security system. This internship provided the opportunity to obtain more knowledge about security incident learning in a healthcare organisation in China and their support enabled us to conduct an exploratory industrial case study.

The redacted hospital was a tertiary level hospital in China and had the highest level of maturity in terms of healthcare information systems. As a tertiary level hospital, the security and reliability of the health information system were highly important. Failure to prevent security incidents can have negative impacts on organisation's critical ability to function.

3.2 Healthcare security compliance regulation

The security management of Chinese healthcare organisations was subject to compliance regulation through security standard GB/T22239 (Information security technology - Baseline for classified protection of information system) [45]. The guidance used a five level information security classification system. Organisations were required to comply with the GB/T22239, by achieving an appropriate level. For example, the guidance of the health industry information security level protection issued by the Ministry of Health of the Peoples Republic of China requires that health

information systems and related units should be self-examined in accordance with GB/T22239. In particular, the tertiary level hospital needed to achieve at least the third security level characterised in GB/T22239 [46]

3.3 Organisational security culture and awareness

The hospital had included security training in the staff induction and this was mandatory. It included the training on how to properly handle patients' private information and how to apply appropriate data protection protocols. However, there were no refresh training sessions for the staff. Employees are not provided with accessible information security materials to update their knowledge probably because information security is not a priority for healthcare professionals [47]. Comparing to the healthcare professionals, the IT professionals got additional training. They were encouraged to attend IT professional training courses and get certifications. The hospital also held security incident sharing sessions for training purposes as part of the incident response follow-up activities. In addition, the organisation has a stated aim of achieving a secure operation by following the security standards [45]. Administrative actions will be taken against the employees who violated the security policies. However, they arguably did not have activities to promote good security practices such as rewarding staff for good security behaviour [48, 49].

3.4 Security incident handling process

Most of the incidents in the hospital were due to hardware failures, human errors (e.g. not following the correct procedures), and policy violation (e.g. the illegal use of USB devices). Hardware failures can usually be solved very quickly either by fixing the technical problem or by replacing it. Business procedure based human errors are always difficult to solve. It took long time to find out what goes wrong at which level.

As opposed to separated responsibilities [24, 26] in handing security incidents and general incidents, the redacted hospital had the IT department responsible for handling all incidents. The IT department treated security incidents equally as general incidents. When a security incident happened, it was logged through phone calls to the IT department. Phone call was the primary way used to report incidents. The IT department also provided a walk in service for incident reporting. Almost all the incidents were reported through phone calls. The redacted hospital did not have an electronic incident logging system to manage incidents, and the work was all paper based.

After incident notification, the severity level of the security incident was then decided according to different severity levels defined by the organisation. The severity levels were defined according to the incidents' impacts on services and reputation. Low severity incidents referred to those that affected only a small part of internal systems, and did not have direct impacts on patients, for example if there was only one end user computer down and this failure would not propagate to affect other parts of the system. High severity incidents referred to those that were critical to the systems' ability to function, with high severity of risk, and impacts on patients, such as the crashing of a critical business function. It also included the incidents that could damage the organisation's reputation, for example the release of patients' private information. A post-incident review was then followed for the high severity incidents. Informal meetings were also held to disseminate the lessons learned to different stakeholders.

3.5 Organisational structure and participants

The hospital had two main divisions, which were medical division, and administrative division. They report to the general director of the hospital. IT department was part of the administrative division. Five IT professionals worked in this department consisting

of four IT engineers and one IT manager. All of them were involved in daily incidents response and handling. To comprehensively understand incident learning within the organisation, we interviewed people from different job roles which included ten healthcare professional (nurses and doctors) and five IT professionals. We have chosen these roles because healthcare professionals are the majorities handling medical records and IT professional are the key personnels dealing with incidents.

The sample was limited by our desire to conduct detailed and focused interviews with key individuals in healthcare organisations. Healthcare and IT professionals within hospitals and medical centres faced an increasing array of demands and requests that left little opportunity to participate in these studies. We were, therefore, extremely grateful for their participation in the qualitative feedback sessions that were documented in this part of the paper.

3.6 The study process

This study adhered to the BPS ethical guidelines, and had been approved by the FIMS ethics committee of the University of Glasgow (ref: CSE01243). The participants completed the consent form before starting the study. Participants were invited to fill in the background questionnaire. This collected the demographic information including job position, gender, education background, years of working experience and experience with security incident handling. We conducted semi-structured interviews with each participant individually in this study. We had chosen this approach instead of group interviews because the participants were reluctant to share their own attitudes towards security with their colleagues. They feel more comfortable to have private conversations.

As suggested by NIST, SANS, and ISO/IEC 27035, the main activities in incident learning are incident knowledge gathering, dissemination and knowledge feedback. We thus focused on three main themes for this interview,

- Incident knowledge gathering
- Incident knowledge dissemination.
- Incident knowledge feedback.

We were not allowed to record the conversations due to the sensitivity of the research themes. Therefore, we took field notes during the interview. After the study, a summary based on the field notes was generated and sent to the informants for confirmation and acceptance within one hour. This was to validate the information's accuracy and completeness. All confirmations were returned by the participants. The results can be accessed and were analysed by the first author only.

4. Results

This section presented the major themes in the data. The findings were grouped according to the research themes. The data was further cross-referenced with the collected document for triangulation [50]

4.1 Background questionnaire

The healthcare professionals who participated in this study, included four doctors (males) and six nurses (females). Their working experience ranges from two to eight years. The educational background of the nurses was at high school or undergraduate levels. All of the doctors had bachelor's degree or above. Among the healthcare professionals, two nurses and one doctor had been involved in the security incident handling process. The rest of them had no experience with security incidents. Five IT professionals participated in this study. Four of them

were IT engineers (one female and three males) and one of them was an IT manager (male). The IT engineers had two to four year's experience and the IT manager had eight years working experience. The educational background ranged from high school to masters. All of the IT engineers had experience with security incident handling.

4.2 Incident response and knowledge gathering

Incident response was handled differently for incidents with different severity levels. For low severity incidents, a security engineer was assigned to the incident till the incident was solved or mitigated. For high severity incidents, an incident response team was formed, which included the IT manager, at least two IT professionals and other people involved in this incident. Knowledge gathering was also different for incidents with different severity levels.

4.2.1 Low severity incident

The handling of low severity security incidents focused more on technical aspects to recover business functions, and placed less emphasis on knowledge gathering of the lessons learned from those incidents. This is evidenced by the following statements provided by the participants from different job roles,

Health Professional: "... for low severity incidents, we inform the IT department ... they solve them very quickly and leave ... we are not very much involved ..."

Security Manager: " ... the business function is the most important, everyone must prioritise it, to turn the system back to normal."

Security Engineer: " ... we can close case when the problem was solved... I sometimes keep technical notes for these low severity incidents, ... but we are not required to do so."

We can see that the health professional who had reported the incident was not involved in the knowledge gathering procedure. The incident handling details were

either not documented or partly documented in the redacted hospital. Based on observations, the hospital did not conduct reviews for low severity incidents. From documents review, we did not find a written requirement in their security management procedures about gathering incident knowledge for low severity incidents.

4.2.2 High severity incident

The handling of high severity incidents was more comprehensive. A security incident team was formed to investigate the incidents. There was a formal process to gather and generate incident knowledge. A review occurred for every high severity incident. Meetings were held to gather information about the incident investigation and mitigation.

Security Manager: " ... for an administrative purpose, we require the incident response team to produce incident reports following severe security incidents..."

Security Engineer: " ... we will have meetings to review those [high severity] incidents and elaborate details about the causes and solutions taken to solve this issue..."

Health Professional: " ... for low severity incidents ... , ... we are not very much involved ... However, for high severity incidents, we are asked to describe details about what we have done in handling the incidents ..."

Health Professional: " ... report how we have discovered the incident, how we have tried to respond to the incident, incident reporting ..."

We can see that the redacted hospital had made some efforts to collect incident information from the staff involved in high severity incidents. The health professional who had reported the incident was also engaged in the knowledge gathering procedure. Lessons were documented and there was a post-incident report generated after the incident. After reviewing their incident reports, we found these reports included information such as business impact, causal analysis and remedial actions. The number

of pages of incident reports reviewed ranged from 7 pages to 60 pages depending on the complexity of the incidents. The report described a complete story about how the incident had happened, incident reporting, analysis, and mitigation.

4.3 Information dissemination

4.3.1 Low severity incident

For low severity incidents, security engineers randomly kept technical notes about the knowledge obtained from the incident handling process. However, they were for personal use only and were not shared with others. This is supported by the following statement,

Security Engineer: " ... I sometimes keep technical notes for future reference ... , ... might be helpful if I encounter the same problem next time ..."

When reviewing those notes, we found they were documented in a free style way either using tables or pure texts. The hospital did not have a systematic way to document and manage learning for low severity incidents, hence created further difficulties in disseminating this knowledge.

4.3.2 High severity incident

For high severity incidents, lessons learned were disseminated through department meetings within the organisation. Security engineers were responsible for incident knowledge dissemination. However, they were unsure whether this knowledge dissemination was effective,

Security Engineer: " ... some incidents contain complicated technical details, I try to explain but I am unsure to what extent they (healthcare professionals) can understand..."

Security Engineer: “ ... it's not easy to communicate technical terms ... , ... stories are most interesting and people like them ...”

Incident dissemination in such flexible manner caused troubles. The healthcare professionals complained about the clarity and the lack of incident knowledge being distributed. Healthcare professionals who had not been involved in the incidents claimed that, mitigation.

Health Professional: “ ... sometimes in departments meeting, security engineers showed up to discuss a security incident ... about how it happened and handled, to be honest, i am not quite sure I can understand them all, I will still need their [security engineers] help ... when I encounter a similar one in the future.”

Health Professional: “... they [security engineers] tell the story about an incident, sometimes using technical terms ... I don't think I can completely digest.”

As mentioned earlier, the organisation produced post-incident reports for high severity incidents. These reports were for administrative purposes and were hardly accessible by people outside the incident response team. Even if these reports were made available, they were still hardly usable. Employees who had seen the reports found it difficult to digest as they contained comprehensive inter-related information. This is supported by the statement of a healthcare professional who had seen the incident reports,

Health Professional: “… the document is so difficult to read, a lot of background information ... everything is mixed together ...”

Based on the analysis above, the information dissemination of the high severity incidents was ineffective. This is due to the complicated nature of the incident itself and ineffective communication between the security engineers and the healthcare professionals.

4.4 Lessons learned feedback

Lessons learned should ideally be used to inform the improvements of security management. Throughout the analysis of qualitative data collected, we were trying to search for evidence on how lessons learned from previous incidents had fed back to security management procedures.

For low severity incidents, there were only occasional informal knowledge feedback activities performed by the security engineers. As mentioned, they took technical notes for handling similar incidents that may happen in the future, but these were not shared with each other. A statement from a security engineer had demonstrated an understanding of the importance in incident knowledge feedback.

Security Engineer: " ... when a similar incident re-occur, I always go back to check previous notes. They are useful, if everybody can share this information ... we can learn from each other's experience and save efforts ..."

The healthcare professionals were also aware of the importance of incident learning and suggested to include incident case study examples in the organisation's security training courses.

Security Engineer: " ... should consider including some [incident] examples in the security training courses ..."

The security manager had a deeper understanding of incident knowledge feedback and linked security lessons with security management procedures.

Security Manager: " ... lessons learned is important to prevent similar incidents in the future, there might be some generic similarities between those incidents ..."

Security Manager: " ... the real causes might be somewhere in the security procedure itself, that a procedure makes people repeat mistakes."

We can see that, the IT professionals were aware of the importance of lessons learned feedback, however, the hospital did not effectively communicate learning of

lessons with the security management policies/guidelines/standards. When examining the incidents reports, we found that these had not stated clearly whether the incidents were caused by inappropriate implementation or the lack of relevant policies/guidelines/ standards, or whether the lessons learned had led to the revision of policies/guidelines/standards. The whole incident response process lacked of a mechanism to feed back lessons to the security management procedures.

5. Discussion

Based on the analysis in previous sections, the organisation had a relatively complete incident handling procedure including preparation, incident investigation, incident mitigation, post-incident learning, an incident response team [26] as well as rules of incident response according to the incident severity levels. However, we have identified some problems from their incident learning process.

5.1 Incident learning and knowledge gathering

SANS and NIST SP800-61 models suggest to produce a detailed post-incident report following a severe security incident. These reports can be used to assist in handling similar incidents, training new team members and leading to the update of incident response policies and procedures [26]. Examples can be found online such as the VA data loss incident reports [1, 2]. In our case study, the redacted hospital had a documented requirement in their security procedure to generate post incident reports documenting business impact, in-depth causal analysis and remedial actions for high severity incidents. Incident reporters were also involved in the knowledge gathering procedure. For low severity incidents, the redacted hospital seemed to focus more on technical aspects to recover business functions, and placed less emphasis on knowledge gathering. Security engineers randomly took technical notes for personal use but these notes was not shared with others. Incident reporters were not very much engaged. This indicated poor collaborations between the incident handler and the incident reporter. This findings is also shared by Ahmad [24, 25] and Tondel [31] According to Cook,

critical incidents were caused by ignorance of low impact incidents and all incidents should be used for incident learning [51]. This was not occurring in the redacted hospital. Ineffective knowledge gathering tends to result in the waste of the knowledge generated in the incident handling process [24]. The findings were consistent with Ahmad's case studies in financial organisations [24, 25]. However, our study was placed in a healthcare context and the target group included not only IT professionals but also healthcare professionals. The importance of information security for different job roles is usually different [52]. This provided us with diversified perspectives from different participants.

5.2 Information dissemination

As suggested by NIST, SANS and ISO 27035, lessons learned about an incident should be disseminated through formal reports, emails, newsletters, meetings and presentations to management [26, 33]. The organisation did not have a systematic way to document and manage low severity incidents. This created difficulties in disseminating lessons learned. For high severity incidents, lessons learned were disseminated through department meetings, however, incident learning was not communicated effectively to the healthcare professionals. Although a detailed post-incident report was produced, it was hardly accessible by people outside the incident response team. Moreover, healthcare professional complained about the lengthy textual reports and found them difficult to digest. The reports were written from an administrative perspective rather than an incident knowledge sharing perspective [37] We can see that incident dissemination in both oral and written were not effective in the organisation. This finding was also share by Ahmad [24, 25] and Tondel [31] This indicated poor communication between incident response teams and other stakeholders. Previous researches [53, 54] argued text alone does not facilitate the communication of security lessons. There is a need for the conversion of post-incident reports into learning documents, which can be easily understood by people in the organisation. Reporting incidents to multiple stakeholders with varying levels of competence and background knowledge was found to be a key challenge for security management.

5.3 Lessons learned to feed into security management procedures

Learning from security incidents can help avoid serious incidents [55] and should ideally improve information security management procedures [24]. NIST, SANS and ISO 27035 has stressed the importance of incident learning and continuously improvements to security management procedures. However, in our case study incidents were not effectively informing improvements of the management procedure in the redacted hospital. The low severity incidents were not properly documented and were not linked to the security procedure. For high severity incidents, the post-incident reports did not clearly document the linkages between lessons learned and security procedures. This raised a question on how to effectively cycle lessons learned into security management procedures. Ahmad [24, 25] proposed a double loop learning model and a dynamic security learning (DSL) process model to address this issue. The DSL process model contains six fundamental processes explaining how learning should occur. It also considers key stakeholders and its linkage with broader organisational aims. It provides a step-by-step procedure-based method to improve incident learning.

We will introduce security assurance modelling framework to address these problems. In particular, our approach aims to provide a unified way to gather incident knowledge and tackle the obstacles of incident reporting to different stakeholders. It also brings in argument theory that allows people to reason about relationships between the lessons learned and security standards. Next section introduces the security assurance modelling framework.

5.4 Incident learning and the assurance modelling framework

This case study has identified the problems in incident learning and the needs for an approach that can provide a unified way to gather security knowledge and can help effectively disseminate incident knowledge to inform security management procedures. We suggest adopting the security assurance modelling framework to address these problems. The following sections introduce the framework and justify how it can address the challenges identified in incident handling process.

5.4.1 Security assurance modelling framework

The security assurance modelling framework is based on argument theory [56, 57]. It presents a documented body of solutions that provides a convincing and valid argument that a specified set of critical claims regarding a system are adequately justified in a given environment [57] As shown in Figure 1, this framework consists of three main components. Security Requirements & Objectives serve as claims (e.g. "Access to sensitive system resources is restricted and monitored"). Security Argument serves as arguments (e.g. "Argument over GB/T22239") and Security Lessons Learned serve as solutions (e.g. "Use encryption, or other effective tool, to protect personally identifiable information stored on removable storage"). The idea is to map security lessons to the organisations security requirements documented in the security standards/guidelines/ policies through using security arguments.

Figure 2 presents a workflow chart on how to apply the assurance modelling framework to link lessons learned with security requirements. The framework starts with top level security claim identification, which can be phrased as "The healthcare information system is secure". It then leads to three directions, which are "Sub requirements needed", "Supporting lessons needed" and "Security arguments needed".

- "Sub requirements needed" is elaborated with different levels of security requirements of the security standards/guidelines/policies. For example, the redacted hospital used GB/T22239. It had a five level information security classification system. This procedure ends until it reaches the level that all sub-requirements of the security standards/guidelines/policies are added to the framework.

- "Supporting lessons needed" is elaborated with the security lessons identified from the incidents. The security lessons that were not covered or addressed by

the security standards can be added to the framework. These security lessons can compliment the current security standards. Some of the security lessons might conflict with existing security standards, then an argument needs to be developed to deal with the conflictions. This procedure ends until all the lessons learned are added to the framework.

- "Security arguments needed" typical deal with the conflictions between the lessons learned and the existing security standards. It can also be used to document the stakeholder's subjective comments towards the security incidents and the security standards. This feedback can also enrich the organisations security standard. This procedure ends until all the arguments development have completed for this framework.

We can see that this framework captures security requirements, lessons learned as well as the stakeholders subjective comments towards the incident. It also provides a way to link security lessons to the security requirements through security arguments. The implementation of this framework can be supported by the graphical notations such as Goal Structuring Notations (GSN) or Claims-Argument-Evidence (CAE). These notations have been widely adopted in security areas \cite{53, 58-61} to develop security requirements. They capture lessons learned and security requirements at different levels of abstraction and provide structured ways to represent security assurance models. The following sections will elaborate on how it can help address the obstacles in security incident learning identified in this case study.

5.4.2 Incident gathering and Assurance modelling

In the case of the redacted hospital, we have identified the organisations' weaknesses in security knowledge gathering and representation. They did not have a structured way to

gather incident knowledge for low severity incidents. Incident report documented for high severity incidents are not for incident preventing and learning purpose. The assurance modelling framework can be applied to address these problems. This is based upon previous researches into the application of this approach to gather and represent security lessons from different data sources, including news articles, money penalty reports and other security incident reports [37, 62]. In particular, it gathers security lessons and classified them according to different levels of technical and managerial security controls. We suggest the redacted hospital follow this framework to gather security incident knowledge. However, questions remains on how security engineers can apply this technique to gather this information during incident handling process in an industrial setting.

5.4.3 Incident dissemination and assurance modelling

We also identified the redacted hospital's weaknesses in disseminating security incident learning. Our results showed that security engineers in the organisation had realised the importance in sharing lessons learned for low severity security incidents rather than taking freestyle notes for their own reference. Security incident reports generated for high severity incidents were found to be difficult to digest and can hardly be used for an incident learning purpose. There a need of an effective way to present incident knowledge that can facilitate incident knowledge dissemination. Security assurance modelling framework can serve this purpose as it was found to be able to effectively communicate security incidents [37, 54]. It can be applied to convert incident reports and represent lessons learned in a structured manner. Another challenge identified from the case study was how to report incidents to multiple stakeholders with varying levels of competence and background knowledge. The security assurance modelling framework can represent security incidents at different levels of abstractions, however,

the level of details need to be scalable and adjusted to fit into the needs of people from different job roles.

5.4.4 Cycle back security knowledge and assurance modelling

This case study showed that the redacted hospital has placed an imbalanced focus on the technical aspects and maintenance of business continuity, and did not leverage opportunity to reuse the security lessons to inform security management procedures for future prevention. Incident knowledge was presented in either a freestyle way or lengthy incident reports had resulted in the difficulties to cycle incident knowledge back to the security management procedures. The assurance modelling framework can be used to address this problem. It links security lessons with different levels of security requirements defined in the security policies/guidance/standard/regulations. Through mapping security lessons to the security requirements, it allows the users to track which security requirement goes wrong at which level and whether there is a need to update the existing security management procedure. This idea can be supported by similar research work in the area of security assessment, where assurance modelling framework has been used to evaluate a security standard, the Common Criteria [63, 64]. Through capturing and constructing security arguments, it revealed 121 issues in a standard that has already been subjected to several rounds of ad hoc reviews. The results showed that the assurance modelling framework was able to detect the incompleteness and weaknesses of the security standards [63].

Recall that in section 3.2, the security management of Chinese healthcare organisations is subject to compliance regulation through security standard GB/T22239. However, security standard is not always perfect and has been criticised as they are validated by appealing to common practise and authority only, which is not a sound basis. The assurance modelling approach can be adopted to cycle back incident

knowledge to inform the improvement of security management procedures. However, questions remain on how security engineers can apply this technique to ensure a continuous improvement of the existing security standard/guidelines informed by the incidents.

6. Conclusions and future work

Lessons learned from security incidents should ideally inform the improvements of organisation's security management procedures. However, previous case studies in financial organisations showed that lessons learned had not been effectively learned. To explore this issue, we conducted a case study in a healthcare organisation.

Through semi-structured interviews with healthcare and IT professionals and reviews of their existing incident handling documents, we found that the organisation placed an imbalanced focus on technical aspects rather than collecting incident knowledge. The organisation did not have a structured way to gather incident knowledge and had not effectively disseminated incident learning for both high severity and low severity incidents. Incident knowledge had not been effectively fed back and led to the changes of security management procedures. To the best of our knowledge, there have not been existing case studies about security incident response and learning in healthcare organisations. This paper contributed to a better understanding of current challenges in incident learning in healthcare organisations.

As different from existing case studies, our target group included not only IT professionals but also healthcare professionals. This provided us with diversified perspectives from different job roles. Non-IT professionals' engagement in incident response is also essential for incident response. We found that healthcare professionals were more engaged in high security incidents then low security incidents. They preferred to have incident case studies in staff security training course. A key challenge

for security management we identified is how to report incidents to multiple stakeholders with varying levels of competence and background knowledge.

To address those issues, we have suggested the assurance modelling framework. As different from Ahmad's step-by-step learning model, our approach aims to provide a unified way to gather incident knowledge and tackle the obstacles of incident reporting to different stakeholders. It also brings in the theory of arguments that allow people to reason about linkage between the lessons learned and security management standards. Moreover, we have discussed the suitability of this approach in tackling the current challenges in security incident learning in healthcare. Future work should expand on these sections on the evaluation of this approach in an industrial setting. Future work should also consider stakeholders from other administrative job roles such as patients registration and finance.

This paper researches into incident learning within the organisation. From a broader perspective, security lessons should be exchanged across different organisations as similar security incidents can happen in different organisations. There are some initiatives to encourage incident exchange between organisations. UK has launched the Cyber Security Information Sharing Partnership (CISP) to help government and industry on cyber security threats vulnerabilities exchange [66]. European Network and Information Security Agency (ENISA) requests member states to report security incidents to enable the exchange of lessons from incidents [66]. There is a need of a structured framework to exchange security lessons. Assurance modelling framework suggested in this paper provided a structured manner to gather, disseminate and feed back incident knowledge. Our research provided the basis for future research into incident knowledge exchange between organisations.

However, assurance modelling framework alone cannot address all the obstacles in incident learning. It needs to be aligned with other methods such as double loop organisational learning, dynamic security learning (DSL) process model and security checklist to improve organisations' incident learning capabilities.

Acknowledgements

The authors would like to thank the Scottish Informatics and Computer Science Alliance (SICSA) for funding this research. The authors would like to thank Professor Marie-Pierre Gagnon from Laval University for the advisory support of this article.

References: see the journal's instructions for authors for details on style

[1] U. V. A. Administration, Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans, Vol. Report No. 06-02238-163, 2006.

[2] U.V.A. Administration, Administrative Investigation Loss of VA Information VA Medical Center Birmingham, AL, Vol. Report No. 07-01083-157, 2007.

[3] I. C. Office, ICO fines NHS Surrey for failing to check the destruction of old computers, http://www.ico. org.uk/news/latest_news/2013/ico-issues-nhs-surrey-monetary-penalty-of-200000 [Online: accessed 18-Nov-2013] (2013).

[4] C. E. Healthcare, Shenzhen Hospital Dataloss Incident, http://www.chinaehc.cn/index.php?option= com_content&view=article&id=1937:2010-04-01-09-38-35&catid=15:medical-reforming& Itemid=15 [Online: accessed 18-Nov-2013] (2008).

[5] Symantec, Internet Security Threat Report 2013,Vol.18, Symantec Corporation, 2013.

[6] Symantec, Internet Security Threat Report 2014, Vol.19, Symantec Corporation, 2014.

[7] R. T. Mercuri, The HIPAA-potamus in health care data security, Communications of the ACM 47 (7) (2004) 25–28.

[8] A.Appari, M.E.Johnson, Information security and privacy in healthcare: current state of research, International Journal of Internet and Enterprise Management 6 (4) (2010) 279–314.

[9] V. Baskaran, K. Davis, R. K. Bali, R. N. Naguib, N. Wickramasinghe, Managing information and knowledge within maternity services: Privacy and consent issues, Informatics for Health and Social Care 38 (3) (2013) 196–210.

[10] S. A. Ebad, E. S. Jaha, M. A. Al-Qadhi, Analyzing privacy requirements: a case study of healthcare in saudi arabia, Informatics for Health and Social Care (0) (2014) 1–17.

[11] J. Kuzma, Web vulnerability study of online pharmacy sites, Informatics for Health and Social Care 36 (1) (2011) 20–34.

[12] T. Porteous, C. Bond, R. Robertson, P. Hannaford, E. Reiter, Electronic transfer of prescription-related information: comparing views of patients, general practitioners, and pharmacists., The British Journal of General Practice 53 (488) (2003) 204.

[13] C. S. Gadd, L. E. Penrod, Dichotomy between physicians' and patients' attitudes regarding EMR use during outpatient encounters., in: Proceedings of the AMIA Symposium, American Medical Informatics Association, 2000, p. 275.

[14] L.Wardman, Patients knowledge and expectations of confidentiality in primary healthcare: aquantitative study, British Journal of General Practice 50 (460) (2000) 901–902.

[15] P.Chhanabhai,A.Holt, Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures, Medscape General Medicine 9 (1) (2007) 8.

[16] G.Perera, A.Holbrook, L.Thabane, G.Foster, D.J.Willison, Views on health information sharing and privacy from primary care practices using electronic medical records, International journal of medical informatics 80 (2) (2011) 94–101.

[17] C. P. Waegemann, IT security: developing a response to increasing risks, International journal of bio-medical computing 43 (1) (1996) 5–8.

[18] I. C. Office, Belfast trust fined £225,000 following data breach, http://www.ico.org.uk/news/latest_ news/2012/belfast-trust-fined-225000-after-leaving-thousands-of-patient-records-in_ disused-hospital-19062012 [Online: accessed 18-Nov-2013] (2012).

[19] I. C. Office, NHS trust fined £325,000 following data breach, http://ico.org.uk/news/latest_news/ 2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients/ -and-staff-01062012 [Online: accessed 18-Nov-2013] (2013).

[20] I. C. Office, Sensitive details of NHS staff published by trust in Devon, http://ico.org.uk/news/latest_ news/2012/sensitive-details-of-nhs-staff-published-by-devon-trust-06082012 [Online: accessed 18-Nov-2013] (2013).

[21] J.Hadgkiss, Computer security incident handling, step-by-step, The SANS Institute,1997.

[22] K. Scarfone, T. Grance, K. Masone, Computer security incident handling guide, NIST Special Publication 800 (61) (2008) 38.

[23] P.Shedden,A.Ahmad,A.Ruighaver, Organisational learning and incident response: promoting effective learning through the incident response process, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, 2010.

[24] A. Ahmad, J. Hadgkiss, A. B. Ruighaver, Incident response teams–challenges in supporting the organisational security function, Computers & Security 31 (5) (2012) 643–652.

[25] A. Ahmad, S. B. Maynard, G. Shanks, A case analysis of information systems and security incident responses, International Journal of Information Management 35 (6) (2015) 717–723.

[26] T.Grance, K.Kent, B.Kim, Computer security incident handling guide, NIST Special Publication(2004) 800– 61.

[27] L. Mei, Y. Ling, A study on issues and strategies concerning the IT-based security system for whole people health, China Science & Technology Resources Review 4 (2010) 009.

[28] C.-D. Wang, W.-B. Yang, S.-G. Ju, Research and implementation of electronic health record signature system based on ces, Computer Engineering 16 (2010) 103.

[29] BS7799, Information security management, BS7799, part 1: code of practice for information security management, 1999.

[30] S.Mitropoulos, D.Patsos, C.Douligeris, On incident handling and response: Astate-of-the-art approach, Computers & Security 25 (5) (2006) 351–370.

[31] I.A.Tøndel, M.B.Line, M.G.Jaatun, Information security incident management: Current practice as reported in the literature, Computers & Security (2014).

[32] C.Hove, M.Tårnes, Information security incident management: an empirical study of current practice.

[33] S. Northcutt, Computer Security Incident Handling: Step by Step, a Survival Guide for Computer Security Incident Handling, Sans Institute, 2001.

[34] N. Direct, National framework for reporting and learning from serious incidents requiring investigation, 2010, http://www.nrls.npsa.nhs.uk/resources/?entryid45=75173 [Online: accessed 18-Nov-2013].

[35] I.C.Office,NHSSurreyc/odepartmentofhealthregionallegacymanagementteam,DataProtectionAct1998 monetary penalty notice, 2013, http://ico.org.uk/enforcement/~/media/documents/library/Data_ Protection/Notices/nhs-surrey-monetary-penalty-notice.pdf [Online: accessed 18-Nov-2013].

[36] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, Handbook for computer security incident response teams (csirts), Tech. rep., DTIC Document (2003).

[37] Y.He, C.Johnson, Generic security cases for information system security in healthcare systems, IET, 2012.

[38] A.Greenough, H.Graham, Protecting and using patient information: the role of the caldicott guardian, Clinical medicine 4 (3) (2004) 246–249.

[39] M.Wei, X.Xue-guo, Discussion of patients' confidentiality in sharing electric medical records, Soft Science of Health 3 (2009) 034.

[40] J. Xian-shan, Security control of computer-based patient record, Information of Medical

Equipment 2 (2006) 008.

[41] P. Shen, X.-y. Hu, S.-g. Zhang, D.-j. Du, Informationalized characteristics of medical records management and risk prevention, Journal of Medical Postgraduates 10 (2009) 021.

[42] Y. Cangzhou, L. Zhongkan, Z. Qishan, A security scheme for electronic medical record systems, Computer Engineering 9 (2004) 050.

[43] X.Gao,J.Xu,G.Sorwar,P.Croll,Implementationofe-healthrecordsystemsande-medicalrecordsystemsin china, The International Technology Management Review 3 (2) (2013) 127–139.

[44] B. S. Alhaqbani, Privacy and trust management for electronic health records, Queensland University of Technology, 2010.

[45] GB/T22239-2008 information security technology - base line for classified protection of information system, AQSIQ/SAC (2008).

[46] M. of Health of People's republic of China, Guidance on the classified protection of information system by ministry of health, 2011, http://www.gov.cn/gzdt/2011-12/09/content_2016113.htm [Online: accessed 18-Nov-2013].

[47] E.Vaast, Dangeris in the eye of the beholders: Social representations of information systems security in healthcare, The Journal of Strategic Information Systems 16 (2) (2007) 130–152.

[48] J.Leach, Improving user security behaviour, Computers & Security 22(8) (2003)685–692.

[49] J. M. Stanton, K. R. Stam, P. Mastrangelo, J. Jolton, Analysis of end user security behaviors, Computers & Security 24 (2) (2005) 124–133.

[50] B.J.Oates, Researching information systems and computing, Sage, 2005.

[51] D.L.Cooke, Learning from incidents, in: 21st System Dynamics Conference, NYC, NewYork, 2003.

[52] P.K.AKSU,N.S ¸,KITAPC ¸I,R.O¨.C ¸ATAR,L.KO¨KSAL, G.MUMCU, An evaluation of information security from the users perspective in turkey, Journal of Health Informatics in Developing Countries 9 (2).

[53] Y.He,C.Johnson,K.Renaud,Y.Lu,S.Jebriel,Anempiricalstudyontheuseofthegenericsecuritytemplatefor structuring the lessons from information security incidents, in: Proceedings of the 6th International Conference on Computer Science and Information Technology, 2014, pp. 178–188.

[54] Y.He, C.Johnson, Y.Lu, A.Ahmad, Improving the exchange of security arguments in security incident reports: Case studies in the privacy of electronic patient records, in: The 8th IFIP WG 11.11 International Conference on Trust Management, 2014.

[55] C. Melara, J. M. Sarriegui, J. J. Gonzalez, A. Sawicka, D. L. Cooke, A system dynamics model of an insider attack on an information system, in: Proceedings of the 21st International Conference of the System dynamics Society, 2003, pp. 20–24.

[56] T.Govier, A Practical Study of Argument Enhanced Edition, Cengage Learning, 2013.

[57] J. Go´rski, Trust casea case for trustworthiness of IT infrastructures, in: Cyberspace Security and Defense: Research Issues, Springer, 2005, pp. 125–141.

[58] A. Goodger, N. Caldwell, J. Knowles, What does the assurance case approach deliver for critical information infrastructure protection in cybersecurity?, in: System Safety, incorporating the Cyber Security Conference 2012, 7th IET International Conference on, IET, 2012, pp. 1–6.

[59] J. Goodenough, H. Lipson, C. Weinstock, Arguing security-creating security assurance cases, rapport en ligne □(initiative build security-in du US CERT), Universite´ Carnegie Mellon (2007).

[60] J.L.Vivas, I.Agudo, J.Lo´pez, A methodology for security assurance-driven system development, Requirements Engineering 16 (1) (2011) 55–73.

[61] C. B. Weinstock, J. B. Goodenough, Towards an assurance case practice for medical devices, Tech. rep., DTIC Document (2009).

[62] Y.He, C.Johnson, K.Renaud, Y.Lu, S.Jebriel, An empirical study on the use of the generic security template for structuring the lessons from information security incidents, in: Computer Science and Information Technology (CSIT), 2014 6th International Conference on, IEEE, 2014, pp. 178–188.

[63] P.J.Graydon,T.P.Kelly, Using argumentation to evaluate software assurance standards, Information and Software Technology 55 (9) (2013) 1551–1562.

[64] P. Graydon, I. Habli, R. Hawkins, T. Kelly, J. Knight, Arguing conformance, Software, IEEE 29 (3) (2012) 50–57.

[65] GOV.UK, Government launches information sharing partnership on cyber security, 2013, https://www.gov. uk/government/news/government-launches-information-sharing-partnership-on-cyber-security [Online: accessed 18-Nov-2013].

[66] D.C.Dimitra Liveri,L.Dupr, Technical guideline on reporting incidents article 13A implementation, European Network and Information Security Agency (2011).

Figure 1. The adjusted assurance modelling framework.

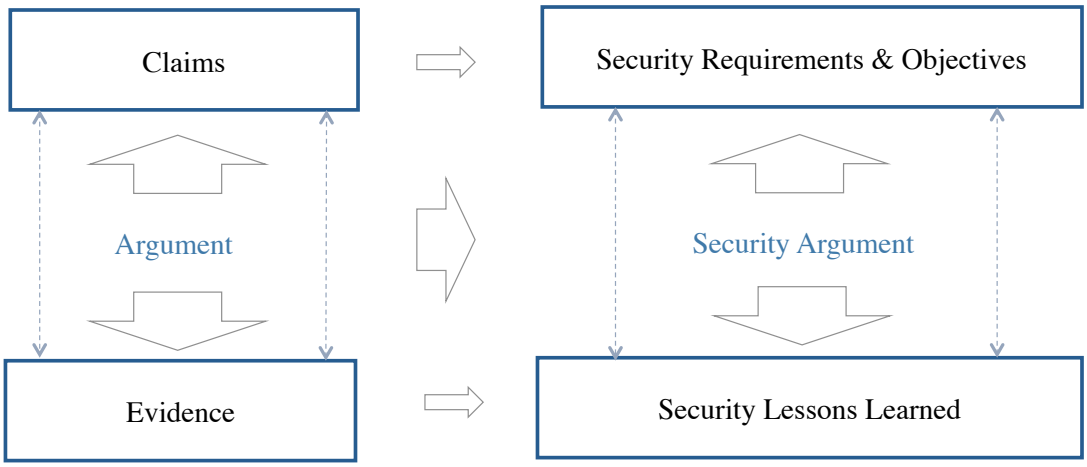

Figure 2. Workflow on feeding back lessons to security management procedure using assurance modelling framework.